Implementasi Metode Discovery Pada Game Edukasi Keamanan Jaringan Komputer

Anteng Widodo
Program Studi Sistem Informasi, Fakultas Teknik, Universitas Muria Kudus
E-mail : antengwidodo@gmail.com

ABSTRACT Nowadays, the innovative learning is needful in learning process. Some methods are applied to achieve the maximum result of learning. The modern learning paradigm put the teacher in certain place as not one only the learning sources. But unhappily, the learning method of computer network security is used at present disposed linier from the teacher to the student or teacher dominated learning. It is boring and not interesting for the students. Besides the learning of computer network safety is not effective without the practice and comprehensive facilities and infrastructure. The first approach conducting to solve the previous problem is using discovery learning method which the students can create and innovate something to solve the given problem. The second approach is the game simulation, which by the simulation can solve the problem of incomprehensive facilities and infrastructure. The third approach is game action, this approach can solve the unattractive learning method of computer network security. Based on the previous three problems, and conducting the approach to solve the problem by implementing and testing, will make the learning the computer network safety more effective, the practice of computer network safety can be done with incomprehensive facilities and infrastructure, and make the learning of computer network security more attractive.
Keywords : Discovery Learning Methods, Game, Computer Network Security

ABSTRAKSI Saat ini pembelajaran yang bersifat inovatif sangat diperlukan dalam proses pembelajaran. Berbagai metode telah diterapkan untuk mencapai hasil pembelajaran yang lebih maksimal. Paradigma pembelajaran modern menempatkan guru bukan satu-satunya sumber belajar. Namun sayangnya, metode pembelajaran keamanan jaringan komputer yang digunakan saat ini cenderung bersifat linier dari guru ke murid atau *teacher dominated learning*. Hal ini tentunya membosankan dan tidak menarik, terlebih lagi pada siswa.
Disamping itu pembelajaran keamanan jaringan komputer kurang efektif jika diajarkan tanpa praktek serta memerlukan sarana dan prasarana yang lengkap. Pendekatan pertama yang dilakukan untuk mengatasi masalah diatas adalah dengan metode pembelajaran *discovery* dimana siswa dapat berkreasi atau berinovasi untuk mengatasi permasalahan yang diberikan. Pendekatan kedua dengan game simulasi, dimana dengan simulasi dapat mengatasi persoalan sarana prasarana yang tidak lengkap. Pendekatan ketiga adalah *game action,* pendekatan ini untuk mengatasi metode pembelajaran keamanan jaringan komputer yang tidak menarik.
Dari ketiga masalah diatas, dan dilakukan pendekatan untuk mengatasi permasalahan tersebut yang diimplementasikan dan diuji, maka pembelajaran keamanan jaringan komputer bisa efektif, praktek keamanan jaringan komputer dapat dilakukan dengan sarana dan prasarana yang tidak lengkap dan metode pembelajaran keamanan jaringan komputer bisa menarik.
Kata kunci : metode pembelajaran discovery, keamanan jaringan komputer

1.1 Pendahuluan

Saat ini pembelajaran yang bersifat inovatif sangat diperlukan dalam proses pembelajaran. Paradigma pembelajaran modern menempatkan guru bukan satu-satunya sumber belajar. Siswa dapat belajar dari sumber belajar di sekitarnya. Tidak ada model pembelajaran yang tepat dalam segala situasi dan kondisi. Pemilihan model pembelajaran harus disesuaikan dengan memperhatikan kondisi siswa, sifat materi pembelajaran, fasilitas-media yang tersedia. Pembelajaran jaringan komputer idealnya diberikan secara teori dan praktek dengan bobot praktek yang lebih besar. Menurut Du[1] yang dikutip dari Denning, *computing* akan terlihat tak bernyawa bahkan terlihat mati ketika proses pengambilan gambar tanpa praktek. Pendapat Denning tersebut dipertegas juga oleh Du[1] yang dikutip dari Irvine, bahwa praktek keamanan jaringan sangat efektif untuk keberhasilan pembelajaran keamanan jaringan komputer. Penyiapan peralatan praktek yang biasa disebut dengan laboratorium jaringan komputer tentunya memerlukan biaya yang mahal. Hal ini juga diungkapkan oleh Benzel yang menyatakan bahwa dalam rangka riset keamanan jaringan yang menghubungkan sistem jaringan akan terkendala oleh mahalnya dalam menyiapkan, membangun dan mendesain infrastruktur laboratorium [2].
Dari hasil penelitian pendahuluan, dengan responden sebanyak 40 siswa kelas XI SMK Muhammadiyah Kudus 1 April sampai dengan 11 Juni 2009, diperoleh hasil sebagai berikut : 22,5% respondent menyatakan bahwa nilai ulangan keamanan jaringan komputer diatas

KKM, sedangkan sisanya, 77,5% menyatakan sebaliknya, yang berarti sama dengan atau dibawah KKM (data ini didukung oleh nilai hasil ulangan harian keamanan jaringan komputer yang diperoleh dari guru mata pelajaran). Selanjutnya yang berkaitan dengan model pembelajaran kemanan jaringan komputer 87,5% responden menyatakan kesulitan dalam memahami pelajaran keamanan jaringan komputer yang disampaikan oleh guru. Sedangkan 12,5% sisanya menyatakan tidak mengalami kesulitan. Kemudian bagaimana respon siswa terhadap metode pembelajaran keamanan jaringan komputer yang selama ini dilakukan. Dari 40 responden, 17,5% menyatakan tertarik dan 82,5% tidak tertarik. Menurut Greitzer[3] yang dikutip dari Bruner, Hermann dan Johnson, bahwa dalam pendekatan konvensional, komunikasi dan bahan pembelajaran terletak pada instruktur atau guru. Beberapa tahun kemudian terjadi perubahan yang terinspirasi dari metode belajar *discovery* dan metode belajar aktif atau metode belajar mandiri atau otonom. Pendekatan pembelajaran yang digunakan dalam pembelajaran keamanan jaringan komputer adalah metode *discovery*. Pendekatan instruksional ini memberikan solusi untuk melengkapi atau mengganti pendekatan pembelajaran secara tradisional dengan pengalaman belajar secara aktif seperti bermain peran, simulasi, atau latihan bersama kelompok belajar secara mandiri, dan jenis lainnya dengan memerlukan pemikiran kritis atau kreatif. Penyiapan laboratorium jaringan komputer untuk praktek pembelajaran keamanan jaringan komputer yang membutuhkan biaya mahal dapat digantikan dengan simulasi. Menurut Ma[4] yang dikutip dari Shin dan Parush , simulasi adalah tiruan percobaan yang nyata. Untuk menampilkan pembelajaran agar lebih menyenangkan, maka penyampaian materi dan latihan dapat disajikan dengan menggunakan teknologi animasi serta *game*. Menurut Rubijesmin[5] yang dikutip dari Aquilera, *game* simulasi dapat membantu dalam perkembangan semua kemampuan intelektual dan pemikiran *logic*. Menurut Rubijesmin, *genre action* di Malaysia lebih disukai siswa dari pada *genre game* yang lain dengan prosentase 23% siswa laki - laki diatas umur 12 tahun dan siswa perempuan dengan prosentase 35% siswa dengan umur diatas 12 tahun .

1.2 Rumusan Masalah

Dari uraian latar belakang diatas maka rumusan masalah dari penelitian ini adalah : materi keamanan jaringan komputer kurang efektif jika diajarkan ke siswatanpa praktek,kurang menarik,dan memerlukan sarana dan prasarana yang lengkap.

1.3 Batasan Masalah

1. Masalah-masalah keamanan jaringan meliputi : virus,ddos dan spam
2. Jenis-jenis virus dan perilakunya tidak disebutkan secara spesifik hanya penanggulangan dan cara mengatasinya secara global.

1.4 Tujuan

Membuat game untuk mensimulasikan pembelajaran keamanan jaringan komputer dengan metode discovery .

1.5 Manfaat

1. Dapat membantu siswa untuk memudahkan pemahaman, menarik dan tidak membutuhkan sarana dan prasarana yang tidak lengkap
2. Memberikan pengembangan teori yang berkaitan dengan game bergenre simulasi

2.1 Metode discovery

Proses pembelajaran harus dipandang sebagai suatu stimulus atau rangsangan yang dapat menantang peserta didik untuk merasa terlibat atau berpartisipasi dalam aktivitas pembelajaran. Peranan guru hanyalah sebagai fasilitator dan pembimbing atau pemimpin pengajaran yang demokratis, sehingga diharapkan peserta didik lebih banyak melakukan kegiatan sendiri atau dalam bentuk kelompok memecahkan masalah atas bimbingan guru. Metode *discovery* merupakan metode yang lebih menekankan pada pengalaman langsung. Pembelajaran dengan metode penemuan lebih mengutamakan proses dari pada hasil belajar. Penggunaan metode *discovery* ini guru berusaha untuk meningkatkan aktivitas siswa dalam proses belajar mengajar. Sehingga metode *discovery* memiliki keunggulan sebagai berikut:

1. Teknik ini mampu membantu siswa untuk mengembangkan, memperbanyak kesiapan, serta panguasaan ketrampilan dalam proses kognitif atau pengenalan siswa.
2. Siswa memperoleh pengetahuan yang bersifat sangat pribadi atau individual sehingga dapat kokoh atau mendalam tertinggal dalam jiwa siswa tersebut
3. Dapat meningkatkan kegairahan belajar para siswa.

2.2 Keamanan Jaringan Komputer

Menurut Wang (Wang, 2009), fungsi dari keamanan jaringan adalah menyediakan kerahasiaan, intregritas, *non-repudiation* dan berguna menjaga ketersediaan data yang ditransmisikan dalam jaringan publik maupun

jaringan lokal. Konsep data dalam konteks keamanan jaringan memiliki arti yang luas yaitu setiap obyek yang dapat diproses atau dijalankan oleh komputer adalah data. Dengan demikian, kode sumber, kode executable, file dalam berbagai format, pesan email, music digital, digital grafis dan video digital termasuk dalam kategori data. Data hanya boleh dibaca, ditulis atau diubah oleh pengguna yang sah dalam artian bahwa individu ataupun organisasi yang tidak berhak tidak diperbolehkan untuk mengakses data tersebut.

3.1 Metode Discovery Untuk Keamanan Jaringan Komputer

Pada penelitian ini, metode *discovery* diterapkan pada tokoh utama untuk mengatasi permasalahan yang terjadi pada komponen-komponen keamanan jaringan komputer.
Tabel berikut menjelaskan penerapan metode *discovery* dalam *game* ini.

Level	Musuh	Pilhan Tool	Rule Action	Kondisi Musuh
PC	Virus	Anti virus IDS Spamassasin	Jika musuh = virus dan tool = anti virus	Virus mati
			Jika tool ≠ anti virus	Virus tidak mati
Server web	Virus Ddos	Anti virus IDS Spamassasin	Jika musuh = virus dan tool = anti virus	Virus mati
Level	Musuh	Pilihan Tool	Rule Action	Kondisi Musuh
Server web	Virus Ddos	Anti virus IDS Spamassasin	Jika tool ≠ anti virus	Virus tidak mati
			Jika musuh = Ddos dan tool = IDS	Ddos mati
			Jika musuh = Ddos dan tool ≠ IDS	DDos tidak mati
Mail Server	Virus Ddos Spam	Anti virus IDS Spamassasin	Jika musuh = virus dan tool = anti virus	Virus mati
			Jika tool ≠ anti virus	Virus tidak mati
			Jika musuh = Ddos dan tool = IDS	Ddos mati
			Jika musuh = Ddos dan tool ≠ IDS	DDos tidak mati
			Jika musuh = spam dan tool = spamassasin	Spam mati
			Jika musuh = spam dan tool ≠spamassasin	Spam tidak mati

Dari tabel diatas dapat dibuat activity diagram untuk level mail server (untuk level *personal computer* dan *server web* hampir sama), sebagai berikut:

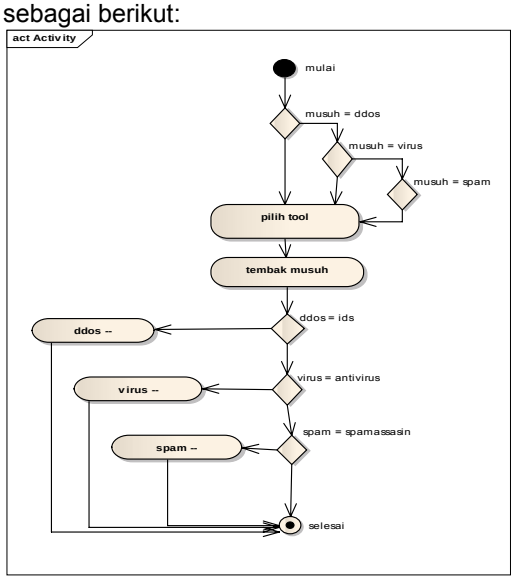


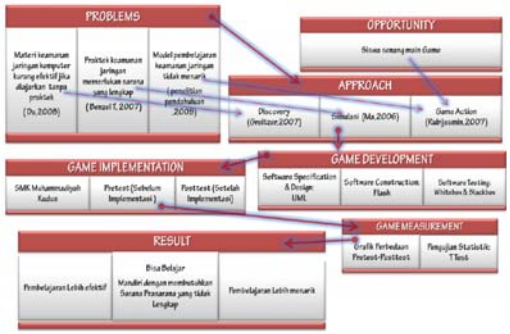
Diagram *activity* diatas terlihat bahwa tokoh utama dihadapkan pada permasalahan pada jaringan komputer, selanjutnya tokoh utama harus memilih tool yang sesuai untuk mengatasi permasalahan tersebut. Sehingga tahapan dalam penerapan metode *discovery* dalam *game* ini menjadi :

1. Tahapan identifikasi permasalahan, terdapat tiga buah permasalahan dalam keamanan jaringan komputer yang harus diselesaikan yaitu virus, ddos dan spam.
2. Tahapan berinovasi mengatasi permasalahan, disini terdapat tiga buah tool untuk mengatasi permasalahan yaitu tool antivirus, *Intrusion Detection System* dan

Spamassasin. Tokoh utama diberikan kebebasan memilih tool untuk mengatasi permasalahan.

3. Tahapan melihat hasil mengatasi masalah, tokoh utama akan melihat hasil berupa permasalahan yang dihadapi akan semakin berkurang jika tool sesuai dengan permasalahan yang ada pada jaringan komputer tersebut. Disini tokoh utama atau pemain diharapkan dapat menarik kesimpulan dengan benar yaitu jika salah memilih tool maka permasalahan tidak dapat diatasi.

3.2 Kerangka Masalah



Gambar 3.1 Kerangka masalah

4 Implementasi dan Hasil

Metode implementasi yang diterapkan kepada user selaku pengguna melalui tahapan-tahapan implementasi adalah sebagai berikut :

1. Menetapkan item-item kuesioner yang nantinya dijadikan sebagai parameter penilaian penelitian,
2. Observasi lapangan untuk menentukan lembaga pendidikan yang dapat dijadikan sebagai tempat penelitian,
3. Melakukan survei awal terhadap 20 responden siswa yang sedang belajar untuk mendapatkan data sebelum implementasi (konvensional) melalui pengisian kuesioner oleh siswa (responden),
4. Penerapan *game* sebagai alat bantu pembelajaran,
5. Melakukan survei untuk mendapatkan data setelah implementasi *game*
6. Melakukan analisa hasil pengukuran penelitian.

4.1 Pengukuran *Game*

Kuesioner diisi oleh responden sebanyak 20 responden. Kuesioner dibagi menjadi dua kali yaitu pada saat sebelum menggunakan *game* yang dibuat, serta setelah menggunakannya.

t-Test: Paired Two Sample for Means		
	Variabel 1	*Variabel 2*
Mean	27.4	32.65
Variance	2.673684211	0.976315789
Observations	20	20
Pearson Correlation	0.51469894	
Hypothesized Mean Difference	0	
Df	19	
t Stat	-16.65684037	
P(T<=t) one-tail	4.29947E-13	
t Critical one-tail	1.729132792	
P(T<=t) two-tail	8.59893E-13	
t Critical two-tail	2.09302405	

Dari tabel diatas dapat dilihat bahwa t tabel (t *critical one-tail*) bernilai 1,729132792 sedangkan t hitung (t *Stat*) bernilai -16,65684037. Terlihat bahwa terjadi perbedaan signifikan. Berarti terdapat perbedaan yang signifikan pula antara sebelum dan sesudah implementasi *game*. Berarti penerapan *game* membawa efek positif. Dengan melihat nilai probabilitas, *P-value* adalah 4,29947E-13 lebih kecil dari 0,05 berarti Ho ditolak atau penerapan *game* efektif.

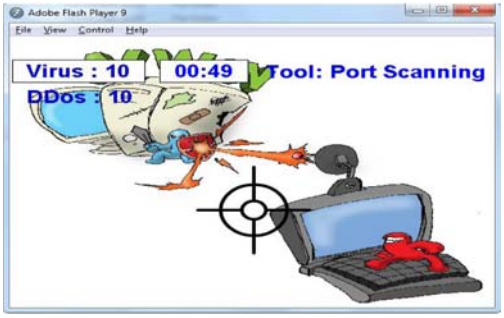
4.2 Tampilan Interface

Secara keseluruhan tampilan interface terbagi dalam tiga buah level :

1. Level *personal computer*
   Pada permainan *personal computer* ini, pemain diharuskan mengalahkan *virus* yang dilambangkan oleh kelelawar yang menyerang sebuah *personal computer*. Virus disini berjumlah sepuluh buah, dan jika pemain berhasil menembak hingga habis dan tidak melampaui batas waktu yang ditentukan maka pemain telah berhasil dalam *level personal computer*.

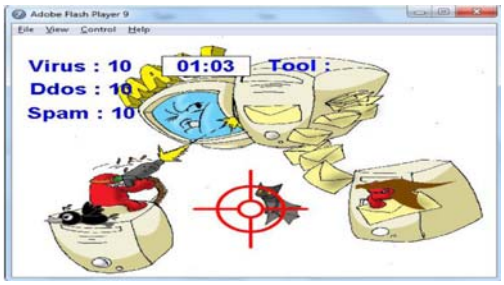
Gambar 1. Tampilan level *personal computer*

2. Level *webserver*
   Pada permainan *web server* ini, pemain diharuskan mengalahkan *virus dan ddos* yang dilambangkan oleh kelelawar dan naga yang menyerang sebuah *web server*. *Virus* disini berjumlah sepuluh buah dan *ddos* juga berjumlah sepuluh buah, dan jika pemain berhasil menembak kelelawar dan naga hingga habis dan tidak melampaui batas waktu yang ditentukan maka pemain telah berhasil dalam *level web server*.



Gambar 2. Tampilan level *webserver*

3. Level *mailserver*
   Pada permainan *mail server* ini, pemain diharuskan mengalahkan *virus, ddos dan spam* yang dilambangkan oleh kelelawar, naga dan burung yang menyerang sebuah *mail server*. Virus,ddos dan spam disini berjumlah sepuluh buah, dan jika pemain berhasil menembak kelelawar, naga dan burung hingga habis dan tidak melampaui batas waktu yang ditentukan maka pemain telah berhasil dalam *level mail server*.



Gambar 3. Tampilan level *mail server*

5 Penutup

5.1 Kesimpulan

Dari ketiga masalah yang diuraikan dalam latar belakang diatas, dan dilakukan pendekatan untuk mengatasi permasalahan tersebut yang diimplementasikan dan diuji, maka pembelajaran keamanan jaringan komputer bisa efektif, praktek keamanan jaringan komputer dapat dilakukan dengan sarana dan prasarana yang tidak lengkap dan metode pembelajaran keamanan jaringan komputer bisa menarik.

5.2 Saran

Ada beberapa hal yang diperlukan sebagai saran pengembangan sistem ini antara lain:

1. Menambah level-level permainan untuk perangkat keamanan jaringan komputer yang lain agar permainan lebih variasi.
2. Menambah soal sebelum pemain mendapatkan tool - tool yang dipergunakan untuk menembak musuh.
3. Menambah pencatatan skor game dan nama yang disimpan dalam *memory* untuk mencatat sejauh mana user telah menyelesaikan tahap permainan.
4. Menambah *Artificial Inteligent* pada *source code* yang ditempatkan pada karakter musuh agar dapat mengenali kondisi tool yang digunakan oleh karakter utama.

DAFTAR PUSTAKA

[1] Du, W. a. (2008). SEED: A suite of instructional laboratories for computer security education. *ACM Journal on Educational Resources in Computing , 8*, 24.

[2] Benzel T, B. R. (2007). Design Deployment and use of the DETER testbed. *In Proceedings of the DETER Community Workshop on Cyber-Security and Test.* Boston.

[3] Greitzer, F. K. (2007). Cognitive Science Implications for Enhancing Training Effectiveness in a Serious Gaming Context. *ACM Journal of Educational Resources in Computing , 7*, 10.

[4] Ma, J. a. (2006). Hands-On, Simulated, and Remote Laboratories: A Comparative Literature Review. *ACM Computing Surveys,Vol.38,Article 7* .

[5] Rubijesmin, A. (2007). Understanding Malaysian students as gamers: Experience. *ACM 978-1-59593-708-7/07/09* .

[6] **Wiji Suhardjo, Bambang Eka Purnama (2013),** *Pemanfaatan Local Area Network Dan Program Netop School Sebagai Media Pembelajaran Interaktif Pada Jurusan Teknik Komputer Jaringan Smk N 1 Klaten, IJNS - Indonesian Journal on Networking and Security - ijns.apmmi.org, IJNS Volume 2 No 3 – Juli 2013 - ISSN: 2302-5700*

[7] *Tina Fajrin, Bambang Eka Purnama,* Analisis Sistem Penyimpanan Data Menggunakan Sistem Cloud Computing Studi Kasus SMK N 2 Karanganyar, Seruni 2012

[8] **Slamet Riyadi, Bambang Eka Purnama (2013),** *Sistem Pengendalian Keamanan Pintu Rumah Berbasis SMS (Short Message Service) Menggunakan Mikrokontroler Atmega 8535, IJNS – Indonesian Journal on Networking and Security, Vol 2 No 4 – Oktober 2013, ijns.org, ISSN: 2302-5700*

[9] *Erlina Cahya Setianingrum, Bambang Eka Purnama,* Sistem Pengaman Brankas Dengan Menggunakan Handphone Berbasis Mikrokontroler AT89S51, Seruni 2013

[10] **Yogi Siswanto, Bambang Eka Purnama,** *Rancang Bangun Aplikasi Mobile Game Edukasi Ilmu Pengetahuan Alam Untuk Anak Kelas VI Sekolah Dasar,* Jurnal Speed Vol 11 No 1 – 2014, ISSN 1979 – 9330